UniReport

6.22

UniReport | Nr. 6 | 8. Dezember 2022 | Jahrgang 55 | Goethe-Universität Frankfurt am Main

Foto: Uwe Dettmar

Seit dem Wintersemester hat sich der Campus Westend noch mehr gefüllt.

Mehr zur Diskussion um den U-Bahn-Anschluss auf S. 2

Editorial des Universitätspräsidenten

Liebe Leserinnen und Leser,

ein bewegtes Jahr neigt sich dem Ende zu. Ich danke Ihnen allen – Studierenden, Lehrenden und Forschenden und Mitarbeitenden in der Verwaltung, – dass Sie mit Ihrem Einsatz die Goethe-Universität mit auf Kurs gehalten haben und wir dadurch viele Herausforderungen erfolgreich bewältigten: Die intensive Arbeit der Clusterinitiativen für die bevorstehende Exzellenzstrategie, die Gründung eines Büros für Nachhaltigkeit, die Rückkehr zur Präsenzlehre; aber auch: die Hilfe für Geflüchtete aus der Ukraine sowie die Bewältigung der aus dem russischen Angriffskrieg resultierenden Energiekrise mit enormen Preissteigerungen auch für die Goethe-Universität. Trotzdem planen wir auch weiterhin, die Präsenzlehre aufrecht zu erhalten. Mit einem Bündel eigener Aktivitäten leisten wir einen signifikanten Beitrag zur Energieeinsparung. Ich freue mich, wenn Sie sich alle daran beteiligen.

Und nun wünsche ich allen Hochschulangehörigen schöne Feiertage und einen guten Start ins neue Jahr, bleiben Sie optimistisch!

Ihr Enrico Schleiff,
Universitätspräsident

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Johann Wolfgang Goethe-Universität | Postfach 11 19 32
60054 Frankfurt am Main | PSDG E+4 |
D30699D Deutsche Post AG | Entgelt bezahlt

www.unireport.info

Wo liegen die Schwachstellen im System?

Informatikprofessorin Prof. Haya Shulman über die Gefahren von Cyberangriffen und wie man Institutionen künftig besser schützt.

UniReport: Frau Prof. Shulman, Sie sind seit letztem Jahr Professorin an der Goethe-Universität, mit einer LOEWE-Spitzenprofessur. Sie sind aber auch Leiterin der Abteilung Cybersecurity Analytics and Defences (CAD) am Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt und Koordinatorin des Forschungsbereichs Analytics Based Cybersecurity am Nationalen Forschungszentrum für Angewandte Cybersicherheit ATHENE. Das ist eine lange Reihe wichtiger Ämter und Funktionen, lassen sich diese gut und produktiv verbinden?

Haya Shulman: Die Kombination ist perfekt. Das Thema Cybersicherheit braucht Interdisziplinarität, und die Goethe-Universität verfügt über eine breite fachliche Exzellenz – nicht nur in der Informatik, sondern auch in der Mathematik, in der Medizin, in der Rechts- und Wirtschaftswissenschaft. Das Fraunhofer-Institut wiederum besitzt Expertise in der Forschung zur angewandten Cybersicherheit. Wir forschen nicht nur zu rein technischen Aspekten, sondern wir kombinieren das auch mit anderen Disziplinen, um für alle damit verbundenen Fragen Lösungen zu finden. Beispielsweise ist die Cyberabwehr ein wichtiges Thema für Deutschland, Europa und auch die USA. Es geht nicht nur darum, die richtige Technologie zu entwickeln, um Cyberangriffe abzuwehren, sondern dabei auch die damit verbundenen rechtlichen und politischen Fragen im Blick zu behalten. Eine in diesem Zusammenhang gerade für Europa wichtige Frage: Wie erkennt man nicht vertrauenswürdige Technologien, auf welcher Basis trifft man da Entscheidungen? Es handelt sich bei Softwareprodukten auch nicht um einen deutschen, sondern um einen europäischen Markt. Es muss also auf europäischer Ebene entschieden werden, welche Produkte nicht mehr verkauft werden dürfen.

Mal ganz laienhaft gefragt: Womit beschäftigen Sie sich in Ihrer Arbeitszeit als Cyber-Expertin hauptsächlich, müssen Sie beispielsweise auch programmieren oder sich testweise irgendwo einhacken?

Ja, sich irgendwo einzuhacken gehört auch zu meiner Arbeit. Normalerweise mache ich eine erste Überprüfung, um Schwachstellen in einem System, im Protokoll oder auf der Plattform zu finden. Danach übergebe ich das an mein exzellentes Team aus wissenschaftlichen Mitarbeitenden und studentischen Hilfskräften. Das Team analysiert und evaluiert dann mit verschiedenen Methoden und in verschiedenen Konfigurationen die Sicherheitslücken. Das Ziel ist es, Probleme in der Sicherheitsarchitektur noch vor den Hackern zu finden und nach Möglichkeit zu beheben.

Man kennt das Prinzip im Alltag: Ein besseres Schloss an der Wohnungstür bietet auch nur begrenzten Schutz, weil der Einbrecher neue Technologien entwickelt, um das Schloss zu knacken, was dann wiederum neue Sicherheitsmaßnahmen erfordert und so weiter. Muss man sich den Kampf um sichere IT-Strukturen ähnlich vorstellen oder hinkt der Vergleich?

Foto: Farideh Diehl/Fraunhofer SIT Darmstadt

Die Frage stellt sich, was eigentlich IT-Sicherheit ist. Diejenigen, die eine Struktur aufbauen, müssen darüber nachdenken, dass und wie es funktioniert. Wer sich mit IT-Sicherheit beschäftigt, ob als Hacker oder als Verteidiger, muss im Gegensatz dazu darüber nachdenken, was schiefgehen kann. Es ist auch sehr spannend, etwas zu finden, das der andere verstecken will oder übersehen hat, also eine Schwachstelle. Damit hat es eher etwas von Schachspielen. Der Unterschied besteht aber darin, dass man sich immer neue Regeln ausdenken muss. Man kann nicht im Voraus berechnen, was der Gegner machen wird, wie und wann er das System angreifen wird.

Fortsetzung auf Seite 12

Fortsetzung von Seite 1

Im Augenblick wird viel darüber diskutiert, dass der Krieg Russlands gegen die Ukraine die Gefahren für die IT-Sicherheit erhöht. Ist die kritische Infrastruktur geschützt, hat man das Thema lange verschlafen? Oder ist es vielmehr nicht auch so, dass es keine absolute Sicherheit geben kann, Staaten und Unternehmen sich nur noch situativ schützen können?

Als „kritisch" im engeren Sinne werden Infrastrukturen definiert, deren Ausfall Folgen für über 500 000 Menschen hätte. Das gab es bislang in Deutschland noch nicht. Man kann sagen, dass es eher unwahrscheinlich wäre, dass eine solche kritische Infrastruktur zufällig Opfer eines Ransom-Angriffs wird. Denkbar wäre hingegen ein staatlich gelenkter Cyberangriff. Beispielsweise wurde ein ukrainischer Stromversorger 2015 Opfer eines staatlich gelenkten Angriffes. Plötzlich waren Millionen Menschen für eine längere Zeit ohne Strom. Bei uns wird die kritische Infrastruktur teilweise mit bereits veralteten Systemen geschützt. Da ergeben sich Lücken im System, für deren Aufspüren es aber schon einer gewissen Expertise bedarf. Man muss sehr genau wissen, um welche Art von Infrastruktur es sich handelt; dafür ist oft auch eine physische Nähe wichtig. Der BND-Präsident hat im letzten Juni gesagt, dass es Anzeichen dafür gebe, dass russische und chinesische Gruppen die deutsche Infrastruktur bereits unterwandert hätten, um Daten abzugreifen und Schadsoftware zu installieren. Im Unterschied zu Ransomware-Angriffen, bei denen sofort klar wird, dass man keinen Zugriff mehr auf das System hat oder dass Daten im Darknet veröffentlicht werden, bemerkt man die Cyberspionage und Vorbereitung zur Sabotage oft nicht – zumindest wenn diese erfolgreich durchgeführt wird.

Florida, USA (2021): Auf einem Tankstellenschild steht »Aus«, weil die Tanks leer sind. Nach dem Cyberangriff und der Abschaltung der Colonial Pipeline Co. wurden die USA mit Benzinknappheit und hohen Benzinpreisen konfrontiert. Foto: Shutterstock/ Hayden Dunsel

Es gibt ja eine Diskussion um Software-Anbieter wie Kaspersky. Man fürchtet im Westen eine Einflussnahme des russischen Staates auf die Virenschutz-Software, aber die Zuständigkeiten der Behörden ist unklar, auch weil sich technische und politische Aspekte überschneiden, oder?

Dazu lassen sich zwei wichtige Fragen formulieren: Wie kommen wir zu sicheren Technologien, und wie können wir nicht vertrauenswürdige Technologien vermeiden? Im September wurde von der Europäischen Kommission ein Entwurf des sogenannten „Cyber Resilience Act" veröffentlicht. Dieser sieht vor, dass Produkte aufgrund von Mängeln vom Markt genommen werden können, wenn dadurch die Sicherheit erhöht werden kann. Wir müssen in Europa gemeinsame Produkte entwickeln, vielleicht so etwas wie einen Airbus für Cybersicherheit schaffen. Das würde Europa weniger abhängig von anderen Ländern machen, insbesondere von solchen, die unsere Werte nicht teilen. Der eine Punkt ist also, selber vertrauenswürdige Produkte herzustellen. Wenn mit dem neuen Cyber Resilience Act nicht sichere Produkte ausgeschlossen werden sollen, stellt sich aber die andere Frage, was man mit der riesigen Menge an schon vorhandener nicht vertrauenswürdiger IT macht. In Deutschland sind die Möglichkeiten begrenzt. Markteingriffe sind nur auf Ebene der EU möglich. Einige westliche Länder haben bereits Listen veröffentlicht, die Hersteller von nicht vertrauenswürdigen IT-Produkten aus Russland enthalten. Es fehlen aber klare politische und rechtliche Regularien. Wir müssen aber auch die Frage beantworten, ob politische Bedenken auch ein Grund sein können, Produkte vom Markt auszuschließen. Bei manchen Herstellern ist gar nicht bekannt, dass sie aus Russland kommen beziehungsweise in enger Beziehung stehen mit russischen Unternehmen. Die Firma Infotecs, die vor Kurzem viel öffentliche Aufmerksamkeit erhielt, ist eine solche Firma, allerdings hat bislang noch kein Betreiber einer kritischen Infrastruktur deren Produkte gekauft. Es stellt sich also die Frage: Wie groß ist die Gefahr, die von der Firma ausgeht?

Auch Hochschulen sind gefährdet, wie einige Fälle der jüngeren Vergangenheit gezeigt haben. Kann man Hochschulen gegen Cyberangriffe ausreichend wappnen?

Hochschulen sind als Organisationen besonders gefährdet: Es gibt sehr heterogene Nutzergruppen, die einen Zugriff auf die IT von außen haben, der nicht gut gesichert ist. Oft richten Fachbereiche oder sogar einzelne Lehrstühle eine eigene Infrastruktur ein. Hier wäre mehr Homogenität wünschenswert. Es gibt also mehr Schwachstellen als in anderen Organisationen, wenngleich es bislang noch nicht viele Cyberangriffe auf Hochschulen gegeben hat. Wir haben jetzt in ATHENE eine Sicherheitsstudie zu allen deutschen Universitäten erstellt. Welche Lücken, welche Schwachstellen gibt es im System, welche Credentials (Berechtigungsnachweise) findet man im Darknet? Ein wichtiges Ergebnis lautet: Es gibt nur wenige überzeugend sichere Unis. Wir haben im Darknet die Login-Daten verschiedener Sektoren von 2018 bis heute angeschaut, die geleakt wurden. Man erkennt, dass die Unis schlechter dastehen als zum Beispiel Organisationen aus den Bereichen IT, KI oder Finanzen. So sind zum Beispiel die verwendeten Passwörter im Durchschnitt von geringerer Qualität. Wir arbeiten gerade an einem Pilotprojekt, in dem es darum geht, eine „Zero Trust Architektur" für wissenschaftliche Einrichtungen aufzubauen. Es handelt sich um das erste Projekt dieser Art in Deutschland. Bei der Zero Trust Architektur handelt es sich um ein schon länger bekanntes Konzept. Konventionelle Sicherheitsarchitekturen sind darauf ausgerichtet, das Netz einer Organisation durch eine Firewall zu schützen, die Angriffe von außen blockieren und filtern soll. Diese Art der Sicherheit bedeutet nun aber auch, dass derjenige, der eine Schwachstelle findet, ins Netz gelangt und dort auf alle Server zugreifen kann. Zero Trust bedeutet demgegenüber, dass man gewissermaßen niemandem traut und jeden Datenzugriff auf Vertrauenswürdigkeit überprüft. In dem Projekt, das Goethe-Universität und Fraunhofer SIT gemeinsam im Rahmen von ATHENE und mit Unterstützung des BMBF durchführen, steht die Frage im Fokus: Welche Technologien passen zu Deutschland? Das Thema hat auch eine hohe strategische Bedeutung für das BMI und für das Auswärtige Amt. Geplant ist, die entwickelte Zero Trust Architektur im Anschluss auch für andere Bereiche zu verwenden.

Die Goethe-Universität ist dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE beigetreten. Prof. Haya Shulman wird die Goethe-Universität im ATHENE-Board vertreten.

Stellt jede/r Nutzer/in der digitalen Hochschulinfrastruktur potenziell eine Gefahr dar, wenn schadhafte Mails nicht erkannt werden? Müssen Mitarbeitende und Studierende dringend sensibilisiert und gegebenenfalls noch stärker geschult werden?

Ja, das ist ein wichtiger Aspekt: Studierende und Mitarbeitende müssen definitiv geschult werden. Man darf auch nicht Auto fahren ohne Führerschein. Wenn man IT verwendet, ohne ein Verständnis der möglichen Gefahren zu haben und zu wissen, wie man diese vermeiden kann, stellt man eine Sicherheitslücke da. Und zwar nicht nur für sich, sondern für das ganze System. Wir haben vor der letzten Bundestagswahl alle im Bundestag vertretenen Parteien in Sachen Cybersicherheit beraten und Workshops angeboten, um die Verantwortlichen zu sensibilisieren: zum Beispiel für gefälschte E-Mails oder Phishing. Wenn jemand damit noch keine Berührung hatte, kann man ihm/ihr das Wissen und die Kompetenzen gut vermitteln.

Fragen: Dirk Frank

ERC Starting Grant für Sebastian Eckart

Physiker Eckart erhält renommierte Förderung des European Research Council zur Erforschung des quantenmechanischen Tunneleffekts

Der „Starting Grant" des European Research Council (ERC) bietet dem Experimentalphysiker Sebastian Eckart vom Institut für Kernphysik der Frankfurter Goethe-Universität die Möglichkeit, mit seiner Arbeitsgruppe physikalisches Neuland zu betreten: „Wir wollen den quantenmechanischen Tunneleffekt in drei Dimensionen betrachten", sagt Eckart. Das war in dieser Form bislang nicht möglich, obwohl der Tunneleffekt seit Jahrzehnten bekannt und gut untersucht ist, da er für die Quantenphysik von fundamentaler Bedeutung ist.

Beim Tunneleffekt durchdringt ein Teilchen eine Potenzialbarriere, die nach den Regeln der klassischen Physik für das Teilchen unüberwindbar ist. Ein analoges Beispiel aus der Mechanik ist ein Ball, der nur über einen Hügel rollen kann, wenn seine Bewegungsenergie höher ist als die potenzielle Energie, die er auf dem Scheitel des Hügels hat. In der Quantenmechanik können Teilchen gelegentlich selbst dann solche Hügel überwinden, wenn sie eigentlich nicht genügend Energie dafür besitzen: Sie bewegen sich dann „einfach" durch den Hügel hindurch, was als „tunneln" bezeichnet wird. Damit ist der Tunneleffekt eines der scheinbar paradoxen Quantenphänomene. Erklären lässt er sich in der Quantenmechanik ungefähr so: Aufgrund der Eigenarten der Quantenphysik sind Teilchen zugleich Wellen. Ein Ausläufer dieser Teilchenwellen kann durch die Potenzialbarriere hindurchreichen und ermöglicht es so dem Teilchen, sich auch jenseits der Barriere zu manifestieren und sich so aus ihr zu „befreien".

„Als zu untersuchendes System nehmen wir einfache Argon-Atome, indem wir einen Strahl aus diesem Edelgas durch unsere Probenkammer schicken", so Eckart. Die für den Tunneleffekt erforderliche Potenzialbarriere besteht aus der elektromagnetischen Anziehung, die der Atomkern auf die Elektronen der Argon-Atome ausübt. Mit extrem starken Laserpulsen, die aus verschiedenen Richtungen auf das Atom treffen und im Kreuzungspunkt eine Intensität von rund einer Billiarde Watt pro Quadratzentimeter erreichen, lassen sich die Elektronen im Atom dann hin und wieder zum Tunneln „überreden". Denn auch wenn die Frequenz der eingestrahlten Laserpulse zu gering ist, um eine direkte Ionisation zu bewirken, so verschieben bei derartigen Starkfeld-Intensitäten die elektrischen Felder der Laserpulse die Elektronen-Teilchenwellen derart, dass der Tunneleffekt möglich wird und bei rund einem Viertel der Atome auch tatsächlich eintritt.

Besonders spannend für das Grundlagenverständnis des Tunneleffekts wird es sein, wie die Eigenschaften der Laserpulse – also ihre Schwingungsrichtungen in allen drei Raumdimensionen – mit den tunnelnden Elektronen wechselwirken. So ist zwar bekannt, dass die Drehimpulse der Lichtteilchen und der Elektronen einen starken Einfluss auf den Tunneleffekt haben können. Gewisse Kombinationen bei den Eigenschaften der Laserpulse und der freigesetzten Elektronen verstärken den Effekt oder schwächen ihn ab. In drei Dimensionen ist dies aber noch nie untersucht worden. Hierzu nutzt Eckart eine Frankfurter Co-Erfindung: das COLTRIMS-Reaktionsmikroskop, mit dem sich atomare Geschehnisse dreidimensional auflösen lassen. Das wird es erlauben, alte und grundlegende Fragen zur Quantenphysik sowie zur Licht-Materie-Wechselwirkung zu beantworten.

Markus Bernards